In the Abstract of the Disclosure:

The following Abstract of the Disclosure replaces all previous Abstracts of the Disclosure:

Technologies to transfer responsibility and control over security from player makers to content authors by enabling integration of security logic and content. An exemplary optical disk (200) carries an encrypted digital video title combined with data processing operations that implement the title's security policies and decryption processes. Player devices include a processing environment (e.g., a real-time virtual machine), which plays content by interpreting its processing operations. Players also provide procedure calls to enable content code to load data from media, perform network communications, determine playback environment configurations (225), access secure non-volatile storage, submit data to CODECs for output (250), and/or perform cryptographic operations. Content can insert forensic watermarks in decoded output for tracing pirate copies. If pirates compromise a player or title, future content can be mastered with security features that, for example, block the attack, revoke pirated media, or use native code to correct player vulnerabilities.